REMARKS

The Examiner's careful consideration of the application is sincerely appreciated. In light of the above amendatory matter and remarks to follow, reconsideration and allowance of this application are requested.

Claim 2 is cancelled. Applicants submit that claims 1 and 120 are clarified so as to obviate the Examiner's objection and 35 U.S.C. 112 rejection. Attached is a marked-up version of changes made to the claims. Thus, claims 1-7 and 120-122 remain in this application.

Claims 1-7 and 120-122, as originally presented, were patentably distinct over the prior art cited by the Examiner, and in full compliance with the requirements of 35 U.S.C. §112. Changes made to these claims are presented, not for the purpose of patentability within the meaning of 35 U.S.C. §§101, 102, 103, or 112, but simply to clarify the invention and to round out the scope of protection to which Applicants are entitled.

Attached hereto is a marked up version of the changes made to the claims in this amendment. The attached page is captioned "**Version with markings to show changes made**". In view of the above amendatory matter and the following remarks, favorable reconsideration of this case is respectfully requested.

Claims 1-5 and 120 are rejected under 35 U.S.C. 102(b) as being anticipated by Wasilewski (U.S. Patent No. 5,420,866). This rejection is respectfully traversed.

Amended independent claim 1 recites:

"A data multiplexing device which multiplexes and transmits transport stream packets of program data comprising a plurality of data elements constructed in the form of transport stream packets, said device comprising:

scramble key generation means for generating a scramble key corresponding to each of said data elements, wherein said scramble key is updated at predetermined intervals; and

scramble means for scrambling said corresponding data element by using a scramble key generated by said scramble key generation means."

Independent claim 120 recites similar limitations.

Fig. 1 of the present invention illustrates a data multiplexing device used for a pay broadcast system. Such a system authorizes only subscribers to watch and/or hear transmitted programs comprised of a plurality of data elements (e.g., video data and audio data). Such a system must scramble programs with scramble keys Ks generated by the broadcast station before transmission and allow only subscribers to descramble the programs to watch and/or hear them.

In order to allow only subscribers to descramble such scrambled programs at the receiver end, scramble keys used in scrambling must be used also for descrambling. To descramble programs transmitted via satellites, these scramble keys must also be transmitted to the receiver end. However, with prior art broadcast systems, an unauthorized recipient is frequently able to obtain these scramble keys and consequently to watch and/or hear all transmitted programs free of charge.

Advantageously, the present invention greatly enhances the security level of the encryption/decryption system, by randomly changing these scramble keys at predetermined intervals. In Fig. 1, a subscriber authorization system 3 generates a different scramble key Ks for each data element contained in a transmitted program. In the example shown in Figure 2, different scramble keys Ks7 through Ks10 are generated and assigned, respectively, to the video data, main audio data, sub-audio data, and private data constituting the fourth program. To optimize security, the subscriber authorization system 3 updates these scramble keys Ks7 through Ks10 at intervals of 4 seconds with a random number generator included in the subscriber authorization system 3.

With regard to claim 1, the Examiner states, in the present Office Action, that "Element 120 of figure 6 [of Wasilewski, the cited reference] shows descrambling, which reads on applicant's scrambling means in claim 1...[and a] descrabler necessitates a key, which would have necessarily been created."

Figure 6 of Wasilewski discloses that "the decryption/descrambling unit 120 employs...ECM's ["Entitlement Control Messages," containing scrambling information] for each elementary stream to decrypt or descramble...each respective elementary stream..." (line 39 of col. 14). However, the reference fails to disclose that such ECM's are periodically updated for security purposes; and the reference nowhere discloses, in particular, "scramble key generation means for generating a scramble key corresponding to each of said data elements, wherein said scramble key is updated at predetermined intervals."

Therefore, withdrawal of the rejections to claim 1 is respectfully requested. For reasons similar to those described above with regard to claim 1, withdrawal of the rejections to independent claim 120, as amended herein, is respectfully requested. Accordingly, Applicants submit, therefore, that the present application is in condition for allowance. An early notice to this effect is respectfully solicited.

Claims 2-5, and 121-122 are dependent from one of claims 1 and 120, and, due to such dependency are distinguishable for the same reasons as the independent claims. Therefore, withdrawal of the rejections to claims 2-5 and 121-122 is respectfully requested.

Claims 1, 2, 4, 6, 7 and 120-122 are rejected under 35 U.S.C. 102(e) as being anticipated by Bando et al. (U.S. Patent No. 5,774,548). This rejection is respectfully traversed.

The Examiner states, in the present Office Action, that '[f]igure 2 of Bando et al. shows two encryption devices working intermediate keys as well as a scrambler."

Brando discloses, in Fig. 2, a system for preventing unauthorized access to a descrambled signal. Although the scrambled signal (TS) is transmitted together with ECM's "obtained by encrypting a scramble key (Ks)..." (line 36 of col. 1), such ECM's are neither changed or updated; and Brando nowhere discloses, in particular, "generating a scramble key corresponding to each of said data elements, wherein said scramble key is updated at predetermined intervals."

Therefore, withdrawal of the rejections to claim 1 is respectfully requested. For reasons similar to those described above with regard to claim 1, withdrawal of the rejections to independent claim 120, as amended herein, is respectfully requested. Accordingly, Applicants submit, therefore, that the present application is in condition for allowance. An early notice to this effect is respectfully solicited.

Claims 2, 4, 6 and 7, and 121-122 are dependent from one of claims 1 and 120, and, due to such dependency are distinguishable for the same reasons as the independent claims. Therefore, withdrawal of the rejections to claims 2, 4, 6 and 7, and 121-122 is respectfully requested.

Claims 1-7 and 120-122 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski in view of Bando et al. This rejection is respectfully traversed.

As described above, neither Wasilewski nor Bando disclose updating scramble keys. Therefore, withdrawal of the rejections to claim 1 is respectfully requested. For reasons similar to those described above with regard to claim 1, withdrawal of the rejections to independent claim 120, as amended herein, is respectfully requested. Accordingly, Applicants submit, therefore, that the present application is in condition for allowance. An early notice to this effect is respectfully solicited.

Claims 2-7, and 121-122 are dependent from one of claims 1and 120, and, due to such dependency are distinguishable for the same reasons as the independent claims. Therefore, withdrawal of the rejections to claims 2-7, and 121-122 is respectfully requested.

In light of the above, Applicants' representative traverses the Examiner's rejections and respectfully submits that the references, alone or in combination do not teach or suggest all of the features of the present invention, as claimed. In view of the foregoing amendments and remarks, it is believed that all of the claims now in this application are patentable over the prior art. Early and favorable consideration thereof is solicited. On the basis of the above amendments and remarks, reconsideration and allowance of this application are respectfully requested.

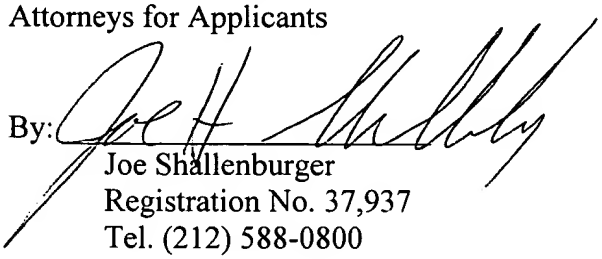
The above statements concerning the disclosures in the cited references represent the present opinion of Applicants' representative and, in the event that the Examiner disagrees, Applicants' representative respectfully requests the Examiner specifically indicate those portions of the respective references providing the basis for a contrary view.

In the event that additional cooperation in this case may be helpful to complete its prosecution, the Examiner is cordially invited to contact Applicants' representative at the telephone number listed below.

The Commissioner is hereby authorized to charge any insufficient fees or credit any overpayment associated with the above-identified application to Deposit Account 50-0320.

Respectfully Submitted,

FROMMER LAWRENCE & HAUG LLP
Attorneys for Applicants

By: 

Joe Shallenburger
Registration No. 37,937
Tel. (212) 588-0800

VERSION WITH MARKINGS SHOWING CHANGES MADE

Claims 1 and 120 have been amended as follows:

1. (Amended) A data multiplexing device which multiplexes and transmits transport stream packets of program data [consisting of] comprising a plurality of data elements constructed in the form of transport stream packets, said device comprising:

[a] scramble key generation means for generating a scramble key corresponding to each of said data elements, wherein said scramble key is updated at predetermined intervals; and

[a] scramble means for scrambling said corresponding [transport stream packet of] data element by using a scramble key generated by said scramble key generation means.

120. (Amended) A data reception device for receiving multiplexed data obtained by multiplexing transport stream packets of program data [consisting of] comprising a plurality of data elements constructed in the form of transport stream packets, said data reception device comprising:

[a] scramble key extract means for extracting from said multiplexed data an enciphered scramble key corresponding to each data element, wherein said enciphered scramble key is updated at predetermined intervals; and

[a] descramble means for descrambling said transport stream packet for each data element contained in said multiplexed data by using a scramble key extracted by said scramble key extract means.